REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed September 13, 2007. Claims 1-32 remain pending in the present application. Reconsideration and allowance of the application and pending claims are respectfully requested.

1. Response to Objection of Claims

Claim 16 has been objected to because of incorrect wording. The claim has been amended to correct the word usage. Withdrawal of the objection is respectfully requested.

2. Response to Rejections of Claims under 35 U.S.C. §102

Claims 1, 10, 14, 17, and 23-26 have been rejected under 35 U.S.C. §102(e) as allegedly being anticipated by *Stone* (U.S. Patent Publication No. 2002/0080964 A1).

a. Claims 1 and 23

As provided in independent claim 1, Applicant claims:

> A method of passing data securely from an originator to a recipient comprising the steps of:
> the originator selecting a condition that the recipient must meet for receipt of the data;
> the originator selecting a trusted party;
> the originator selecting a first key without reference to the condition;
> ***the originator encrypting the data using the first key;***
> ***the originator making the condition, and the encrypted data available to the recipient;***
> ***the recipient providing the trusted party with evidence that it meets the condition;***
> ***the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient, and***
> ***the recipient decrypting the data using the first key.***

(Emphasis added).

Applicants respectfully submit that independent claim 1 is allowable for at least the reason that *Stone* does not disclose, teach, or suggest at least "the originator encrypting the data using the first key; the originator making the condition,

and the encrypted data available to the recipient; the recipient providing the trusted party with evidence that it meets the condition; the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient, and the recipient decrypting the data using the first key," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. For example, material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the watermark removal data to a data carrier, where the watermark removal data is preferably in encrypted form. As such, *Stone* does not disclose a method of passing data comprising at least the steps of "the originator making the condition, and the encrypted data available to the recipient; the recipient providing the trusted party with evidence that it meets the condition; the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient, and the recipient decrypting the data using the first key," as recited in claim 1.

As a result, *Stone* does not anticipate claim 1, and the rejections of claim 1 and claim 23 which depends there from should be withdrawn.

b. Claims 10 and 24

As provided in independent claim 10, Applicant claims:

> A method for an originator to make data available securely to a recipient comprising the steps of:
> the originator selecting a condition that the recipient must meet for receipt of the data;
> the originator selecting a trusted party;
> ***the originator selecting a first key without reference to the condition;***
> ***the originator encrypting the data using the first key, and***
> ***the originator making the condition, and the encrypted data available to the recipient.***

(Emphasis added).

Applicants respectfully submit that independent claim 10 is allowable for at least the reason that *Stone* does not disclose, teach, or suggest at least "the originator selecting a first key without reference to the condition; the originator

encrypting the data using the first key, and the originator making the condition, and the encrypted data available to the recipient," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. For example, material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the watermark removal data to a data carrier, where the watermark removal data is preferably in encrypted form. As such, *Stone* does not disclose a method for making data available securely to a recipient comprising at least the steps of "the originator selecting a first key without reference to the condition; the originator encrypting the data using the first key, and the originator making the condition, and the encrypted data available to the recipient," as recited in claim 10.

As a result, *Stone* does not anticipate claim 10, and the rejections of claim 10 and claim 24 which depends there from should be withdrawn.

c. Claims 14 and 25

As provided in independent claim 14, Applicant claims:

> A method for a recipient to receive data made available securely by an originator, who has selected a trusted party to be involved, comprising the steps of:
> ***obtaining a condition for decryption of the data set by the originator and the data encrypted using a first key generated without reference to the condition and;***
> ***providing the trusted party with evidence that it meets the condition;***
> ***receiving the first key for decryption of the data from the trusted party, and***
> ***decrypting the data.***

(Emphasis added).

Applicants respectfully submit that independent claim 14 is allowable for at least the reason that *Stone* does not disclose, teach, or suggest at least "obtaining a condition for decryption of the data set by the originator and the data encrypted using a first key generated without reference to the condition and; providing the trusted party with evidence that it meets the condition; receiving the first key for

decryption of the data from the trusted party, and decrypting the data," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. For example, material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the watermark removal data to a data carrier, where the watermark removal data is preferably in encrypted form. As such, *Stone* does not disclose a method to securely receive data comprising at least the steps of "obtaining a condition for decryption of the data set by the originator and the data encrypted using a first key generated without reference to the condition and; providing the trusted party with evidence that it meets the condition; receiving the first key for decryption of the data from the trusted party, and decrypting the data," as recited in claim 14.

As a result, *Stone* does not anticipate claim 14, and the rejections of claim 14 and claim 25 which depends there from should be withdrawn.

d. Claims 17 and 26

As provided in independent claim 17, Applicant claims:

> A method for a trusted party to facilitate the passing of data securely from an originator to a recipient, where the originator has selected a condition which the recipient must meet for receipt of the data, and has encrypted the data with a first key generated without reference to the condition, comprising the steps of:
>
> receiving from the recipient evidence that they meet the condition;
>
> ***comparing the evidence against the condition to confirm that the recipient does meet the condition, and***
>
> ***if the recipient meets the condition, providing the first key to the recipient that is capable of decrypting the data.***

(Emphasis added).

Applicants respectfully submit that independent claim 17 is allowable for at least the reason that *Stone* does not disclose, teach, or suggest at least "comparing the evidence against the condition to confirm that the recipient does meet the

condition, and if the recipient meets the condition, providing the first key to the recipient that is capable of decrypting the data," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. For example, material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the watermark removal data to a data carrier, where the watermark removal data is preferably in encrypted form. As such, *Stone* does not disclose a method of passing data comprising at least the steps of "comparing the evidence against the condition to confirm that the recipient does meet the condition, and if the recipient meets the condition, providing the first key to the recipient that is capable of decrypting the data," as recited in claim 17.

As a result, *Stone* does not anticipate claim 17, and the rejections of claim 17 and claim 26 which depends there from should be withdrawn.

e. Claim 23

As provided in independent claim 23, Applicant claims:

> A method of passing data securely from an originator to a recipient comprising the steps of:
> the originator selecting a condition that the recipient must meet for receipt of the data;
> the originator selecting a trusted party;
> the originator selecting a first key without reference to the condition;
> ***the originator encrypting the data using the first key;***
> ***the originator making the condition, and the encrypted data available to the recipient;***
> ***the recipient providing the trusted party with evidence that it meets the condition;***
> ***the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient, and***
> ***the recipient decrypting the data using the first key.***

(Emphasis added).

Applicants respectfully submit that independent claim 1 is allowable for at least the reason that *Stone* does not disclose, teach, or suggest at least "the originator encrypting the data using the first key; the originator making the condition,

and the encrypted data available to the recipient; the recipient providing the trusted party with evidence that it meets the condition; the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient, and the recipient decrypting the data using the first key," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. For example, material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the watermark removal data to a data carrier, where the watermark removal data is preferably in encrypted form. As such, *Stone* does not disclose a method of passing data comprising at least the steps of "the originator making the condition, and the encrypted data available to the recipient; the recipient providing the trusted party with evidence that it meets the condition; the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient, and the recipient decrypting the data using the first key," as recited in claim 1.

As a result, *Stone* does not anticipate claim 1, and the rejection of claim 1 should be withdrawn.

3. Response to Rejections of Claims under 35 U.S.C. §103

Claims 2-9, 11-13, 15-16, 18-22, and 27-32 have been rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Stone* in view of *Yoshiura* (U.S. Patent No. 6,131,162).

a. Claims 2-9

Claim 1 is allowable over the cited art of record for at least the reasons given above. Since claims 8-9 depend from claim 1 and recite additional features, claims 2-9 are allowable as a matter of law over the cited art of record. Further, *Yoshiura* is legally inadequate to remedy the deficiencies of the *Stone* reference.

b. **Claims 11-13**

Claim 10 is allowable over the cited art of record for at least the reasons given above. Since claims 11-13 depend from claim 10 and recite additional features, claims 11-13 are allowable as a matter of law over the cited art of record. Further, *Yoshiura* is legally inadequate to remedy the deficiencies of the *Stone* reference.

c. **Claims 15-16**

Claim 14 is allowable over the cited art of record for at least the reasons given above. Since claims 15-16 depend from claim 14 and recite additional features, claims 15-16 are allowable as a matter of law over the cited art of record. Further, *Yoshiura* is legally inadequate to remedy the deficiencies of the *Stone* reference.

d. **Claims 18-22**

Claim 17 is allowable over the cited art of record for at least the reasons given above. Since claims 18-22 depend from claim 17 and recite additional features, claims 18-22 are allowable as a matter of law over the cited art of record. Further, *Yoshiura* is legally inadequate to remedy the deficiencies of the *Stone* reference.

e. **Claim 27**

As provided in independent claim 27, Applicant claims:

> A computer system for passing data securely from an originator to a recipient comprising a first computer entity associated with the originator, a second computer entity associated with the recipient and a third computer entity associated with a trusted party, there being communication means between the first computer entity and the second computer entity and between the second computer entity and the third computer entity,
>
> ***the first computer entity selecting a condition to be met by the recipient before receipt of the data and a first key generated without reference to the condition, and encrypting the data with that first key, and encrypting the condition and the first key using a public key of the trusted party, and making both available to the second computer entity;***
>
> ***the second computer entity being arranged to forward evidence that the recipient meets the condition to the third computer entity, and***
>
> ***the third computer entity being arranged to compare the evidence with the condition and if satisfied that the recipient meets the condition to provide the first key to the second computer entity for decryption of the data.***

(Emphasis added).

Applicants respectfully submit that independent claim 27 is allowable for at least the reason that *Stone* in view of *Yoshiura* does not disclose, teach, or suggest at least "the first computer entity selecting a condition to be met by the recipient before receipt of the data and a first key generated without reference to the condition, and encrypting the data with that first key, and encrypting the condition and the first key using a public key of the trusted party, and making both available to the second computer entity; the second computer entity being arranged to forward evidence that the recipient meets the condition to the third computer entity, and the third computer entity being arranged to compare the evidence with the condition and if satisfied that the recipient meets the condition to provide the first key to the second computer entity for decryption of the data," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. Material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the data to a data carrier, where the data is preferably in encrypted form. As such, *Stone* does not disclose a computer system comprising at least "the first computer entity selecting a condition to be met by the recipient before receipt of the data and a first key generated without reference to the condition, and encrypting the data with that first key, and encrypting the condition and the first key using a public key of the trusted party, and making both available to the second computer entity; the second computer entity being arranged to forward evidence that the recipient meets the condition to the third computer entity, and the third computer entity being arranged to compare the evidence with the condition and if satisfied that the recipient meets the condition to provide the first key to the second computer entity for decryption of the data," as recited in claim 27.

Further, *Yoshiura* describes a distribution system that encrypts content using the public key of a user of the receiving system. *See* col. 8, lines 60-67. Accordingly, *Yoshiura* fails to cure all of the deficiencies of the *Stone* reference. Additionally, the claimed subject matter recites that a first key of an originator of the data that is being passed is used to encrypt the data and not a key of the recipient.

Therefore, *Stone* in view of *Yoshiura* fail to teach or suggest all of the claimed features, including "the first computer entity selecting a condition to be met by the recipient before receipt of the data and a first key generated without reference to the condition, and encrypting the data with that first key, and encrypting the condition and the first key using a public key of the trusted party, and making both available to the second computer entity; the second computer entity being arranged to forward evidence that the recipient meets the condition to the third computer entity, and the third computer entity being arranged to compare the evidence with the condition and if satisfied that the recipient meets the condition to provide the first key to the second computer entity for decryption of the data," as recited in claim 27.

As a result, claim 27 is patentable over *Stone* in view of *Yoshiura*, and the rejection of claim 27 should be withdrawn.

f. Claims 28-30

Claim 27 is allowable over the cited art of record for at least the reasons given- above. Since claims 28-30 depend from claim 27 and recite additional features, claims 28-30 are allowable as a matter of law over the cited art of record.

g. Claim 31

As provided in independent claim 31, Applicant claims:

> A method of passing data securely from an originator to a recipient comprising the steps of:
>
> the originator selecting a condition that the recipient must meet for decryption of the data; the originator selecting a trusted party having a public key;
>
> the originator selecting a first key without reference to the condition;
>
> ***the originator encrypting the data using the first key;***
>
> ***the originator encrypting the condition and the first key using the public key of the trusted party;***
>
> ***the originator making the condition, and the encrypted data and the encrypted condition and first key, available to the recipient;***
>
> ***upon receipt by the trusted party of the recipient's public key, the encrypted condition and first key, and evidence that the recipient meets the condition, the trusted party decrypts the condition and first key, satisfies itself that the recipient meets the***

condition, provides the first key to the recipient, and the recipient decrypts the data using the first key.

(Emphasis added).

Applicants respectfully submit that independent claim 31 is allowable for at least the reason that *Stone* in view of *Yoshiura* does not disclose, teach, or suggest at least "the originator encrypting the data using the first key; the originator encrypting the condition and the first key using the public key of the trusted party; the originator making the condition, and the encrypted data and the encrypted condition and first key, available to the recipient; upon receipt by the trusted party of the recipient's public key, the encrypted condition and first key, and evidence that the recipient meets the condition, the trusted party decrypts the condition and first key, satisfies itself that the recipient meets the condition, provides the first key to the recipient, and the recipient decrypts the data using the first key," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. Material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the data to a data carrier, where the data is preferably in encrypted form. As such, *Stone* does not disclose a method of passing data comprising at least "the originator encrypting the data using the first key; the originator encrypting the condition and the first key using the public key of the trusted party; the originator making the condition, and the encrypted data and the encrypted condition and first key, available to the recipient; upon receipt by the trusted party of the recipient's public key, the encrypted condition and first key, and evidence that the recipient meets the condition, the trusted party decrypts the condition and first key, satisfies itself that the recipient meets the condition, provides the first key to the recipient, and the recipient decrypts the data using the first key," as recited in claim 31.

Further, *Yoshiura* describes a distribution system that encrypts content using the public key of a user of the receiving system. *See* col. 8, lines 60-67. Accordingly, *Yoshiura* fails to cure all of the deficiencies of the *Stone* reference. Additionally, the claimed subject matter recites that a first key of an originator of the

data that is being passed is used to encrypt the data and not a key of the recipient. Therefore, *Stone* in view of *Yoshiura* fail to teach or suggest all of the claimed features, including "the originator encrypting the data using the first key; the originator encrypting the condition and the first key using the public key of the trusted party; the originator making the condition, and the encrypted data and the encrypted condition and first key, available to the recipient; upon receipt by the trusted party of the recipient's public key, the encrypted condition and first key, and evidence that the recipient meets the condition, the trusted party decrypts the condition and first key, satisfies itself that the recipient meets the condition, provides the first key to the recipient, and the recipient decrypts the data using the first key," as recited in claim 31.

As a result, claim 31 is patentable over *Stone* in view of *Yoshiura*, and the rejection of claim 31 should be withdrawn.

h. Claim 32

As provided in independent claim 32, Applicant claims:

> A method of passing data securely from an originator to a recipient comprising the steps of:
> the originator selecting a condition that the recipient must meet for decryption of the data;
> the originator selecting a trusted party;
> the trusted party generating an asymmetric key pair without reference to the condition and providing the encrypting key of the asymmetric key pair to the originator to act as a first encrypting key;
> the originator providing the condition to the trusted party;
> the trusted party storing the condition and the asymmetric key pair;
> ***the originator encrypting the data using the first encrypting key;***
> ***the originator making the condition, and the encrypted data available to the recipient;***
> ***upon receipt by the trusted party from the recipient of the evidence that the recipient meets the condition the trusted party retrieves the condition and asymmetric key pair from store, satisfies itself that the recipient meets the condition, and provides the decrypting key of the asymmetric key pair to the recipient to act as a first decrypting key, and***
> ***the recipient decrypting the data using the first decrypting key***.

(Emphasis added).

Applicants respectfully submit that independent claim 32 is allowable for at least the reason that *Stone* in view of *Yoshiura* does not disclose, teach, or suggest at least "the originator encrypting the data using the first encrypting key; the originator making the condition, and the encrypted data available to the recipient; upon receipt by the trusted party from the recipient of the evidence that the recipient meets the condition the trusted party retrieves the condition and asymmetric key pair from store, satisfies itself that the recipient meets the condition, and provides the decrypting key of the asymmetric key pair to the recipient to act as a first decrypting key, and the recipient decrypting the data using the first decrypting key," as emphasized above.

Rather, *Stone* describes a process for transferring watermarked material, where it is noted that watermarked material is not the same as encrypted material. Material that has been watermarked is playable, usable, or accessible by a user, whereas content of encrypted material is not accessible by a user until the material is decrypted. Further, *Stone* describes how a buyer of watermark removal data may transfer the data to a data carrier, where the data is preferably in encrypted form. As such, *Stone* does not disclose a method of passing data comprising at least "the originator encrypting the data using the first encrypting key; the originator making the condition, and the encrypted data available to the recipient; upon receipt by the trusted party from the recipient of the evidence that the recipient meets the condition the trusted party retrieves the condition and asymmetric key pair from store, satisfies itself that the recipient meets the condition, and provides the decrypting key of the asymmetric key pair to the recipient to act as a first decrypting key, and the recipient decrypting the data using the first decrypting key," as recited in claim 32.

Further, *Yoshiura* describes a distribution system that encrypts content using the public key of a user of the receiving system. *See* col. 8, lines 60-67. Accordingly, *Yoshiura* fails to cure all of the deficiencies of the *Stone* reference. Additionally, the claimed subject matter recites that a first key of an originator of the data that is being passed is used to encrypt the data and not a key of the recipient. Therefore, *Stone* in view of *Yoshiura* fail to teach or suggest all of the claimed features, including "the originator encrypting the data using the first encrypting key; the originator making the condition, and the encrypted data available to the recipient; upon receipt by the trusted party from the recipient of the evidence that

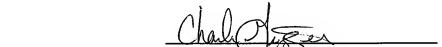
the recipient meets the condition the trusted party retrieves the condition and asymmetric key pair from store, satisfies itself that the recipient meets the condition, and provides the decrypting key of the asymmetric key pair to the recipient to act as a first decrypting key, and the recipient decrypting the data using the first decrypting key," as recited in claim 32.

As a result, claim 32 is patentable over *Stone* in view of *Yoshiura*, and the rejection of claim 32 should be withdrawn.

CONCLUSION

For at least the reasons set forth above, Applicant respectfully submits that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned agent at (770) 933-9500.

Respectfully submitted,



Charles W. Griggers, Reg. No. 47,283